McAfee® Encrypted USB Devices User Guide

McAfee Encrypted USB—Standalone 7.0

McAfee®

COPYRIGHT

Copyright © 2008 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

SAFEBOOT is a registered trademark or trademark of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. Microsoft® and Windows® are registered trademarks of Microsoft Corporation. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Attributions

Refer to the product Release Notes.

CONTACT INFORMATION

Download Site http://www.mcafee.com/us/downloads/

Technical Support http://www.mcafee.com/us/support/

KnowledgeBase Search (includes access to product documentation)

http://knowledge.mcafee.com/

McAfee Technical Support ServicePortal (Logon credentials required)

https://mysupport.mcafee.com/eservice_enu/start.swe

Customer Service

Web

http://www.mcafee.com/us/support/index.html

http://www.mcafee.com/us/about/contact/index.html

Phone — US, Canada, and Latin America toll-free:

+1-888-847-8766 Monday – Friday, 8 a.m. – 8 p.m., Central Time

Contact information for other countries can be accessed online by selecting a link under Worldwide Offices at:

http://www.mcafee.com/us/about/contact/index.html

Contents

Introducing McAfee Encrypted USB Devices 4
About McAfee Encrypted USB Devices 4
Security 5
System requirements 5
Getting started 6
Personalizing a device 6
Choosing and applying a device profile 6
Creating the Administrator account 7
Creating the first user 7
Starting Encrypted USB 7
Installing McAfee Encrypted USB—Standalone 8
Upgrading to McAfee Encrypted USB—Standalone 7.0 8
Accessing the device 9
Locking, unlocking, and disconnecting the device 9
Understanding LED states 10
Saving and opening files 11
Managing users 12
Types of users 12
Creating a user 12
Deleting a user 13
Managing authentication methods 13
Rescuing a user 14
Managing devices 15
Recycling a device 15
Viewing device information 15
Starting programs using the Encrypted USB menu 16
Troubleshooting 17
I cannot eject my device 17
My user name is not in the list for biometric authentication 17
My user name is not in the list for password verification 17
My biometric device will not authenticate my finger 17
Password or biometric access to my device is blocked 18
My device Drive Mappings do not appear 18
Data saved to the read-only partition is not available 18
Appendix: Device policy settings 19
Index 21

Introducing McAfee Encrypted USB Devices

McAfee Encrypted USB Devices are USB (Universal Serial Bus) portable drives that provide different types of security and data encryption. You can personalize and manage a device using McAfee Encrypted USB—Standalone software (referred to as Encrypted USB throughout the rest of the document). Encrypted USB provides step-by-step instructions to help you set up your device and start using it.

For large deployments of McAfee Encrypted USB Devices, use McAfee Encrypted USB Manager—a scalable software solution that lets you control devices throughout their life cycle, from personalization through to delivery to end users and eventual recycling. For more information about McAfee Encrypted USB Manager, contact McAfee.

This chapter provides information about the following:

- About McAfee Encrypted USB Devices
- Security
- System requirements

About McAfee Encrypted USB Devices

The following table provides a brief description about each device. Encrypted USB supports all listed devices.

Table 1-1: McAfee Encrypted USB Devices

Device		Description
	McAfee Zero Footprint Biometric Encrypted USB (formerly SafeBoot for USB Phantom Bio)	▪ Biometric, password, and two-factor security ▪ Built-in Encrypted USB software (no installation required) ▪ Public, private, and read-only disk partitions
	McAfee Zero Footprint Non-Biometric Encrypted USB (formerly SafeBoot for USB Phantom Non-Bio)	▪ Password security ▪ Built-in Encrypted USB software (no installation required) ▪ Public, private, and read-only disk partitions
	McAfee Encrypted USB Hard Disk (formerly SafeBoot for USB Hard Disk)	▪ Biometric, password, and two-factor security ▪ Built-in Encrypted USB software (no installation required) ▪ Public, private, and read-only disk partitions ▪ Available with various hard drive sizes
	McAfee Standard Encrypted USB (formerly SafeBoot for USB Standard)	▪ Flash drive ▪ Password security ▪ Public and private disk partitions ▪ Encrypted USB software available to install

Note: Read-only disk partitions on the following devices can be configured as a regular drive or as a CD-ROM: McAfee Zero Footprint Biometric Encrypted USB, McAfee Encrypted USB Hard Disk, and McAfee Zero Footprint Non-Biometric Encrypted USB. For more information, see “Starting programs using the Encrypted USB menu” on page 16.

Security

Security options vary according to which McAfee Encrypted USB Device you are using. In general, the two main areas of protection for each device include:

1. Access to the device—controlled by the authentication mechanisms available to the device, including biometric (fingerprint), password, and two-factor. Two-factor authentication requires both a biometric and a password to unlock a device.

2. Protection of private data—provided by encrypting the information belonging to each user in private stores and partitions.

McAfee Encrypted USB Devices encrypt private partition data using the FIPS approved AES algorithm (FIPS PUB 197). Data is automatically decrypted when the user opens the file. All devices support the following AES key sizes: 128,192, and 256 bits. However, the default key size for McAfee devices is 256-bit encryption, which is also the only option available with Encrypted USB software. Other options are available through the McAfee Software Development Kit. Encryption keys are unique to each user and are generated each time you create a user.

System requirements

The following list describes the requirements you need to use your device with Encrypted USB. If you are using McAfee Standard Encrypted USB, you must install Encrypted USB on your computer. Other McAfee devices include a pre-installed version of Encrypted USB on the read-only partition of the device.

- A USB port (Type A)
- An operating system that supports USB 2.0 or 1.1 Mass Storage Devices

Operating systems

- Microsoft Windows Vista (Business, Enterprise, and Ultimate Editions)
- Windows Vista 64-bit, Windows XP Professional x64 Edition (support for all devices except McAfee Standard Encrypted USB)
- Windows XP SP1, Windows XP SP2
- Windows 2000 SP4

Web browsers

- Microsoft Internet Explorer 6.0 or Internet Explorer 7.0

Getting started

You must personalize a new or recycled McAfee Encrypted USB Device the first time you use it. For information about recycling a device, see “Recycling a device” on page 15. For McAfee Standard Encrypted USB devices, you must install McAfee Encrypted USB—Standalone before you can personalize the device. If you are using a device with a previous version of Encrypted USB, you can upgrade to the newest version.

This chapter provides information about the following topics:

- Personalizing a device
- Starting Encrypted USB
- Installing McAfee Encrypted USB—Standalone
- Upgrading to McAfee Encrypted USB—Standalone 7.0

Personalizing a device

Encrypted USB starts the personalization process automatically when you plug in a new or recycled device. If autorun is not configured for your computer, you can start Encrypted USB from the read-only partition on the device. Personalizing a device involves three main steps—applying a device profile, creating the Administrator, and creating users.

Choosing and applying a device profile

Device profiles determine the type of authentication method to use, for example biometric, password, or two-factor, and other device policies, such as number of users, password length, biometric and password retry limits and so on. When you apply a device profile, you can choose from two options: Typical, and Custom. The read-only partition size is 80MB (this does not apply to McAfee Standard Encrypted USB) for both options.

Typical

The Typical option uses the main authentication method that is available with the device, for example, fingerprint authentication for biometric devices. It allows one user on the device (not including the device administrator). The Typical option applies the following default authentication settings (if applicable):

- Private partition size equals the total available disk space
- Two Factor authentication: Off
- Biometric Security Level: 1 in 4,500
- Minimum password length: 6
- Biometric Retry Limit: Infinite
- Password Retry Limit: 10

Custom

The Custom option lets you choose the authentication method to use with the device and customize device policies. The policies that are available depend on the type of device you have, for example, biometric or non-biometric. When a device has multiple users, the private partition space is divided equally among all users.

Possible authentication methods include:

- Biometric Only
- Password Only
- Biometric AND Password (Two Factor)
- Biometric OR Password

Possible device policies include:

- Maximum number of users
- Biometric retry limit
- Biometric security level
- Minimum password length
- Password retry limit

Note: For more information about device policy settings, see “Appendix: Device policy settings” on page 19.

Creating the Administrator account

Only the Administrator can perform certain operations on a device, such as adding, removing, and rescuing users. Memorize or store the Administrator password in a safe place. Without the password, you cannot change some device settings.

All new or recycled devices have only one Administrator. The user who personalizes the device determines the Administrator password. For more information, see “Types of users” on page 12.

Creating the first user

After you create the Administrator account, you are automatically prompted to create a user and provide authentication credentials, such as enrolling fingers, creating a password, or both. The authentication method varies according to the device and profile being used. For more information about adding users, see “Creating a user” on page 12.

To personalize a device

1. Plug the device into the USB port of the computer.

   If Autorun does not start Encrypted USB automatically, double-click the Start.exe file from the root directory on the read-only partition.
2. If you just recycled the device, under **Device Management**, click **Personalize Device**.
3. On the **Device Personalization** page, click one of the device profile options.
4. Type the Administrator password in the **Enter password** and **Confirm password** boxes.
5. Complete the instructions on the pages that follow to add user and authentication information.

Note: If you do not complete the personalization process you may have to redo some of the steps the next time you connect the device.

Starting Encrypted USB

Encrypted USB lets you manage users and your device.

To start Encrypted USB

- From the notification area at the far right of the taskbar, click the McAfee icon, and then click the appropriate option from the menu.

  If you are using McAfee Standard Encrypted USB, from the **Start** menu, click **All Programs**, **McAfee**, **McAfee Encrypted USB**, and then click the appropriate option from the menu.

Installing McAfee Encrypted USB—Standalone

McAfee Standard Encrypted USB requires you to install Encrypted USB because it does not have a read-only drive. All other devices have a pre-installed version of Encrypted USB on the read-only partition of the device.

After you install Encrypted USB, you must personalize the device for use. For more information, see “Personalizing a device” on page 6.

To install Encrypted USB

1. Put the CD into the CD-ROM drive of the computer.
2. If Autorun does not start the setup program, you can double-click the **Setup.exe** file from the root directory.
3. Follow the instructions in the Install wizard.

Upgrading to McAfee Encrypted USB—Standalone 7.0

You can upgrade a device that uses a previous version of Encrypted USB software to Encrypted USB 7.0. You must download and unzip the Encrypted USB upgrade package to your computer before you can install it on the device.

Encrypted USB 7.0 allows only one Administrator account per device. If your device currently has multiple users with administrative privileges, these accounts will be maintained when you upgrade the device. However, if you remove an Administrator account you cannot recreate it. For more information about Administrators, see “Creating the Administrator account” on page 7.

To upgrade Encrypted USB

1. Double-click the **SWUpdate.exe** file from the temporary folder to which it was downloaded and unzipped.
2. In the **McAfee Configuration Manager** window, type the Management code for the device in the **Management Code** box.
3. Select the **Manage Read-Only Partition** check box.
4. In the **Read Only Image** box, type the path of the McAfee Encrypted USB—Standalone_7_0 folder located in the temporary folder where the upgrade package was downloaded.

   You can also click the (...) button and browse to the folder.
5. Click **Update**.

Note: The upgrade process automatically resizes the read-only partition if it does not have sufficient disk space for the Encrypted USB 7.0 image. You can override the resize operation by selecting the Override automatic resize check box and typing the maximum size for the read-only partition.

Accessing the device

You can lock the device to ensure that only authenticated users can access it while you are away from the computer. You can also disconnect the device completely to bring the data with you. Light emitting diodes (LEDs) indicate the current state of the device. Once authenticated, you can save files to, and open files from, a private partition. You can also copy data between two McAfee Encrypted USB Devices.

This chapter provides information about the following topics:

- Locking, unlocking, and disconnecting the device
- Understanding LED states
- Saving and opening files

Locking, unlocking, and disconnecting the device

If you leave your device plugged in and unlocked, any user can access your private partition while you are away from the computer.

To lock the device

1 From the notification area, at the far right of the taskbar, right-click the McAfee icon and click **Lock Device**.

If you are using McAfee Standard Encrypted USB, from the **Start** menu, click **All Programs**, **McAfee**, **McAfee Encrypted USB**, and then click **Lock**.

2 If Encrypted USB is already open, on the main page, under **Device Management**, click **Lock Device**.

Tip: You can also lock your device by right-clicking the private partition in a file manager, and then clicking **Eject**.

To unlock the device

1 From the notification area, at the far right of the taskbar, right-click the McAfee icon and click **Unlock Device**.

If you are using McAfee Standard Encrypted USB, from the **Start** menu, click **All Programs**, **McAfee**, **McAfee Encrypted USB**, and then click **Unlock**.

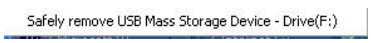
2 If Encrypted USB is already open, on the main page, under **Device Management**, click **Unlock Device**. Follow the prompts in the authentication wizard until the device successfully authenticates you.

Tip: If your device uses only biometric authentication, you can unlock it without starting Encrypted USB by swiping your finger across the fingerprint sensor.

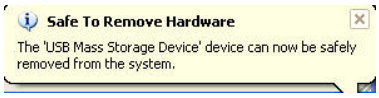
To disconnect the device

1 From the notification area, at the far right of the taskbar, click the **Safely Remove Hardware** icon.

2 Click the message “Safely remove USB Mass Storage Device - Drive (F:); where F is the letter of the drive to which the device is associated in the file manager.



3 When you see the following prompt, you can safely disconnect the device from the USB port.



Caution Disconnecting the device either accidentally or on purpose, without using the safely remove hardware operation, could corrupt the data on the device.

Understanding LED states

All McAfee Encrypted USB Devices except McAfee Standard Encrypted USB use a light emitting diode (LED) to indicate the operational status of the device. The LED states vary depending on the device you are using.

Table 1-1: LED states for devices

State	Description of state
Solid green	Open—if no authentication mechanisms are set, any user can use the device. Unlocked—if users exist, it indicates that the device has authenticated a user.
Flashing green (normal)	The flash frequency is approximately once per second and indicates that the device is waiting for a finger due to one of the following situations: ▪ The device has just been plugged in and is currently locked. ▪ Software has initiated a biometric authentication or enroll operation. ▪ A user has initiated a finger authentication operation for example, by touching the device when it is in the “idle” waiting-for-finger state—see Flashing green slow.
Flashing green (slow)	Indicates that the device is waiting for a finger to authenticate but has been idle for some time.
Flashing red once	Failed fingerprint authentication attempt. The device will go back to waiting for a finger (flashing green normal) after the failed signal finishes.
Flashing LED alternating between red and green	The device is waiting for a finger to authenticate but this is also the last chance to authenticate before biometric access is blocked. The frequency is approximately twice per second.
Flashing red	The device is either powering up or is totally blocked. When totally blocked, no authentication methods are available to unlock the device; this indicates that the device needs to be recycled.
Solid red	The device is locked.
Blue LED	Indicates a data transfer activity for all devices.
Flashing red and blue	The device no longer has valid firmware.

Saving and opening files

You can save files to a private partition that only you can access. The device encrypts data saved to a private partition using the FIPS-approved AES algorithm (does not apply to McAfee Standard Encrypted USB devices). Data is automatically decrypted when you open the file.

Once you authenticate to the device, you can access files on your private partition. If the device is locked and you try to access the private partition the following message displays, “insert a disk into drive H:” where H is the drive letter associated with the private partition.

Note: You cannot save data to the read-only partition.

Managing users

An Administrator can create and delete users. Users can manage their authentication methods by enrolling or deleting fingers, changing their password, or both. You can also rescue users who can no longer authenticate to the device.

This chapter contains information about the following topics:

- Types of users
- Creating a user
- Deleting a user
- Managing authentication methods
- Rescuing a user

Types of users

With McAfee Encrypted USB Devices, you can register two types of users on the device:

- **Administrator**—automatically created by the first user to personalize the device. The Administrator only manages the device and can access the public partition only if it is not disabled. If you are the only device user, you must create both the Administrator account and a user account. If you cannot authenticate to the device with your user account, you can use the Administrator account to rescue users.

  The Administrator can authenticate to the device using only a password. Therefore, it is very important that you remember the Administrator password or store it in a safe place. McAfee Encrypted USB—Standalone automatically prompts you to authenticate as the Administrator to perform tasks that require administrative privileges, such as adding or removing users, rescuing users, and changing the Administrator password.
- **General users**—typical device user who can authenticate to the device and save data to a private partition. Users can change their passwords and update finger enrollments.

Creating a user

Creating a user involves creating a user name and providing authentication details, such as enrolling fingers, typing passwords, or both. You can add a maximum of five users (including the administrator) to any device. When you add users to devices with biometric authentication—McAfee Zero Footprint Biometric Encrypted USB and McAfee Encrypted USB Hard Disk—a maximum of six fingerprint templates can be enrolled among all users.

The Personalization wizard automatically prompts you to create the first user after you create the Administrator account. You can create more users as necessary if your device profile supports multiple users.

To create a user

1 On the main page of **Encrypted USB**, under **User Management**, click **Create User**.

2 Complete the instructions on the **Create User** page to add the user and authentication credentials.

Deleting a user

Only the administrator can remove a user from the device. Once you delete a user, the user's data is permanently lost even if a key recovery system exists.

To delete a user

1 On the main page of Encrypted USB, under **User Management**, click **Delete User**.
2 Complete the instructions on the **Delete User** page to delete the user.

Note: Upgraded devices may have multiple Administrator accounts that were created using a previous version of Encrypted USB. Once you delete an Administrator account, you cannot recreate it. If only one Administrator account remains on the device, you cannot remove this user.

Managing authentication methods

Before you can change your authentication details, such as enroll a finger or change your password, you must authenticate to the device. Otherwise, only an Administrator can change a user's authentication details.

Once you reach the total number of enrolled fingers allowed for the device or your user account, you cannot enroll more.

To enroll a finger

1 On the main page of Encrypted USB, under **User Management**, click **Manage Authentication Methods**.
2 Click **Enroll Fingerprint** and follow the instructions to enroll a new finger.

To delete a fingerprint

1 On the main page of Encrypted USB, under **User Management**, click **Manage Authentication Methods**.
2 Click **Delete Enrolled Fingerprint** and follow the instructions to delete the fingerprint.

Note: If you delete the user's last fingerprint template, and the user is not set up to use password authentication, you will prevent the user from accessing data on the private partition and in the private store unless you reset the user's authentication method. For more information, see "Rescuing a user" on page 14.

To change a password

1 On the main page of Encrypted USB, under **User Management**, click **Manage Authentication Methods**.
2 Click **Change Password** and follow the instructions on the **Change Password** page to create a new password.

If you are using two-factor authentication, the device will prompt you to authenticate using a biometric before opening the **Change Password** page.

Rescuing a user

Rescuing a user resets the user's authentication method by deleting finger enrollments, resetting a password, or both. Users can then enroll fingers and set a password as required. For more information, see "Managing authentication methods" on page 13.

Only an Administrator can rescue a user if you or another user on the device can no longer authenticate to it. For example, you may be prevented from authenticating if you exceed the number of authentication attempts allowed for the device or you forget your password.

If you upgrade your device from a previous version of Encrypted USB, you cannot perform rescue operations for existing device users because there are no backup encryption keys. You can rescue new users who were added after the upgrade process.

To rescue a user

1. On the main page of Encrypted USB, under **User Management**, click **Rescue User**.
2. In the **Password** box, type the Administrator password and click **Next**.
3. If there are multiple users on the device, click the user who cannot authenticate to the device from the **User Name** list and click **Next**.
4. Complete the instructions on the pages that follow to add new authentication information.

Managing devices

Recycling a device removes all users and data from the device. You can also view device information to verify user, device configuration, partition, and version information. McAfee devices (except McAfee Standard Encrypted USB) can be configured so that you can start other programs on your device using the McAfee Encrypted USB—Standalone menu in the taskbar.

This chapter provides information about the following topics:

- Recycling a device
- Viewing device information
- Starting programs using the Encrypted USB menu

Recycling a device

Recycling a device returns it to a default state by deleting all users and authentication mechanisms. All data and security keys are unrecoverable. The Administrator or any user who knows the device management code can recycle a device. The management code option is available if a device has been upgraded from a previous version of Encrypted USB or if the Administrator account is blocked. You must personalize the device after you recycle it. For more information, see “Personalizing a device” on page 6.

To recycle a device

1. On the main page of Encrypted USB, under **Device Management**, click **Recycle Device**.
2. If the Administrator is not the current user, type the Administrator password in the **Password** box and click **Next**.

   Encrypted USB automatically recycles the device.
3. If you want to recycle the device using the management code, under **Quick Links**, click **Recycle using the management code**, and then type the code in the **Management Code** box.

Viewing device information

You can view information about users and the device. All information is read-only.

To view device information

1. On the main page of Encrypted USB, under **Device Management**, click **View Device Information**.

2 On the **Device Information** page, click one of the following categories:

- **User—**provides authentication and partition information for each user, such as the number of finger enrollments allowed, password and two-factor status, and private partition size.
- **Device Settings—**contains biometric and hardware information such as retry limits and security levels, and the device serial number.
- **Disk Partitions—**outlines the overall allocation of disk space on the device.
- **Versions—**lists the version for all software and hardware associated with the device.

Starting programs using the Encrypted USB menu

You can start programs that are installed on your device from the Encrypted USB menu in the taskbar. You can also configure your device to automatically start a program when you plug it in. To start a program automatically the partition on which the program is installed must be configured as a CD-ROM drive.

The Encrypted USB menu supports the autorun of programs from the read-only, public, and private partitions.

To start a program from the Encrypted USB menu

1 From the notification area, at the far right of the taskbar, click the McAfee icon .

2 Select the program from the menu.

Note 1: The ability to disable or enable a menu item depends on the state of the device, such as open, locked, unlocked, or blocked.

Note 2: McAfee Standard Encrypted USB does not use the Encrypted USB menu.

Troubleshooting

If you have problems using your McAfee Encrypted USB—Standalone, you may find a solution in one of the following scenarios. For further technical assistance, contact http://www.mcafee.com/us/support/index.html.

I cannot eject my device

When you try to eject your device from the file manager, you may encounter the following error:

"Cannot Unmount Volume—An error was encountered trying to unmount 'Removable Disk (F:)' Check to make sure there are no open files or windows from that volume."

If you are not an administrator on the computer then this message will always appear and prevent you from ejecting the drive. This is a limitation documented by Microsoft in the following article:

http://support.microsoft.com/default.aspx?scid=kb;en-us;192785

To work around this issue, you can lock the device using Encrypted USB or safely remove the device using the taskbar icon, see "To disconnect the device" on page 9.

My user name is not in the list for biometric authentication

If your user name is not in the list of users when you attempt to authenticate using a biometric, then you either do not have any fingers enrolled, or your biometric access is blocked.

The administrator of your device can unblock biometric access to allow you to enroll fingers. For more information, see "Rescuing a user" on page 14.

My user name is not in the list for password verification

If your user name is not in the list of users when you attempt to authenticate using password verification, then either you do not have a password, or it is blocked. The administrator of your device can set a password for you or unblock your password. For more information, see "Rescuing a user" on page 14.

My biometric device will not authenticate my finger

A device may fail to authenticate a finger if the biometric sensor is damaged, or your fingerprint has aged or has been altered due to environmental factors or injury. If you have extra finger enrollments, you can enroll another finger or delete an existing fingerprint and enroll a new one. For more information, see "Managing authentication methods" on page 13. If the sensor is broken, contact the administrator or McAfee.

Password or biometric access to my device is blocked

You will receive a warning message when you have only one remaining password or biometric attempt left before you reach the retry limit. When you exceed the retry limit, the device blocks you from authenticating to it using that authentication method. You must contact your administrator to unblock your user account. For more information, see “Rescuing a user” on page 14.

My device Drive Mappings do not appear

Sometimes a drive letter for a partition of a McAfee Encrypted USB Device does not get mapped. This occurs when a network drive mapping occupies a letter typically assigned to one of the drives of the McAfee Encrypted USB Device.

If you map a network drive to a resource using the drive letter typically assigned to a McAfee Encrypted USB Device, you will not see the device drive in the file manager window when you connect the device. This problem occurs only if you map the drive while the device is disconnected from the computer. You need to disconnect the mapped network drive. To work around the mapping issue, it is recommended that you re-map the network drive using a drive letter from the end of the alphabet, for example, Z or Y. For more information about this Microsoft network drive issue, see the following Microsoft Web address:

http://support.microsoft.com/?kbid=830238

Data saved to the read-only partition is not available

You cannot save data to the read-only partition of devices. Data saved here is stored in the cache of the Windows file manager. It is deleted when you remove the device. Save data to only your private partition or the public partition (if applicable).

Appendix: Device policy settings

During the Custom personalization process, you can customize device policy settings. The policy settings that are available vary according to the type of authentication the device uses. For more information about personalizing a device or to see a list of default device settings, see “Personalizing a device” on page 6 or “Choosing and applying a device profile” on page 6.

The following table describes each policy setting and indicates the devices to which these options apply.

Table 1-1: Device policy settings

Policy setting	Description	Applicable devices
Number of Users	Total number of users you can add to the device to a maximum of four. This does not include the administrator account.	All devices
Minimum Password Length	Minimum number of characters an end user can specify when creating a valid password.	All devices except McAfee Standard Encrypted USB
Biometric Security Level	Applies to all device users. It is expressed as a False Match Rate (FMR) probability, such as “1 in 10,000”. FMR is the probability that two different fingers are incorrectly matched. A low FMR means higher security because the device requires a closer match between two fingerprints. Therefore, “1 in 10,000” is more secure than “1 in 1,000”. However, a low FMR also means that the device may reject a genuine user because the sensor is less tolerant of small fingerprint deviations due to dirt, improper placement of the finger, and so on. Conversely, a high FMR means the device is less likely to reject a genuine user but more likely to incorrectly match two different fingerprints. If a user has difficulty authenticating to the device at the desired level of security, it is recommended that you also assign the user a password.	▪ McAfee Zero Footprint Biometric Encrypted USB ▪ McAfee Encrypted USB Hard Disk
Retry Limits	A retry limit is the number of failed authentication attempts (either biometric or password) allowed before users are blocked from unlocking the device. For example, a retry limit of one will block users after two failed attempts. Retry limits for both biometric and password authentication can range from 1 to 255, or infinite. It is recommended that you set biometric retry limits higher than password retry limits since biometric authentication failures are not always the fault of the user. When a user exceeds a retry limit while trying to authenticate to the device, the following action occurs:	

Table 1-1: Device policy settings

Policy setting	Description	Applicable devices
	Biometric Retry Limit—All users are automatically blocked from accessing the device using biometric authentication. Password authentication is still available (if applicable). Note: Biometric false rejections (when a genuine user is not validated during an authentication attempt even when using an enrolled finger) can occur with any biometric system. The false rejection rate increases with higher biometric security levels. Therefore, it is recommended that you set a high biometric retry limit to minimize the chances of blocking access to the device for biometric users due to false rejections. Setting a low retry limit can easily result in blocked access, especially if a low False Match Rate (FMR) is set for the biometric security level. See also, Biometric Security Level.	▪ McAfee Zero Footprint Biometric Encrypted USB ▪ McAfee Encrypted USB Hard Disk
	Password Retry Limit—The user who exceeded the retry limit is prevented from using a password to unlock the device. Biometric authentication (if applicable) is still available if the biometric retry limit has not been exceeded.	All devices

Note: For information about setting options beyond what is available with Encrypted USB 7.0, contact http://www.mcafee.com/us/support/index.html.

Index

A

adding
  fingers 13
  first user 7
  users 12
administrative privileges 12
Administrator
  about 7
Advanced profile
  about 19
applications
  starting 16
authentication methods 13

B

biometric
  deleting 13
  enrolling 13
biometric access blocked 18
biometric profiles 6
biometric retry limit
  about 20
biometric security level
  about 19
biometric verification
  troubleshooting 17
blocked
  biometric or password access 18
blue LED 10

C

changing passwords 13
Connector 16
contacting
  McAfee 17
creating
  new password 13
  users 12
creating an Administrator 7

D

data not appearing
  troubleshooting 18
default
  device settings 6
  profile settings 6
deleting
  fingerprints 13
  users 13
devices
  about profiles 6
  adding users 12
  advanced settings 19
  default settings 6
  personalizing procedure
  read-only partition 18
  recycling 15
  rescuing users 14
disconnecting the device 9

E

editing
  passwords 13
ejecting device
  troubleshooting 17
Encrypted USB
  starting 7
  upgrading 8
Encrypted USB menu 5
enrolling fingers 13
enrollment privileges 12
error
  Cannot Unmount Volume 17

F

false match rate 19
fingerprints
  deleting 13
fingers
  enrolling 13

G

general users 12
green LED 10

H

hardware version 15

I

initializing a device
  see personalizing
installing Encrypted USB
  McAfee Standard Encrypted USB 8

L

LED
  blue 10
  flashing green 10
  flashing green normal 10

flashing green slow 10
flashing red 10
solid green 10
solid orange 10
solid red 10
states 10
LED states 10
locking the device 9

M

Management code 6
mapping network drives 18
McAfee
system requirements 5
McAfee Standard Encrypted USB
installing 8
minimum password length
about 19

N

network drives
mapping 18

O

opening files 11
operating systems supported 5
orange LED 10

P

partitions
opening files 11
read-only 18
saving files 11
viewing size 15
password authentication
name not in list 17
password profiles 6
passwords
about retry limits 20
Administrator 7
changing 13
personalizing a device
profiles
about 6
programs
starting 16
public partition size 6

R

read-only partition 5
devices 18
recycling devices 15
red LED 10
removing
devices 9
users 13
rescuing users 14
resetting
user authentication methods 14
retry limits
about 19

S

Safely Remove Hardware operation 9
saving files 11
software version 15
starting Encrypted USB 7
supported
operating systems 5
Web browsers 5
system requirements 5

T

technical support 17
troubleshooting
biometric verification 17
blocked access to device 18
data not appearing 18
ejecting device 17
finger authentication failed 17
network drive issue 18
password access blocked 17
unsafe removal event dialog 17
user name 17
two-factor profile 6

U

unlocking the device 9
unplugging the device 9
unsafe removal event dialog 17
upgrading Encrypted USB 8
user name (biometric)
not in list 17
user name (password)
not in list 17
users
adding 12
adding the first time 7
administrators 12
changing authentication methods 13
definition of 12
general 12
removing 13
rescuing 14
viewing number of 15

V

version number 15
viewing
device configuration 15
partition information 15
user information 15
version information 15

W

Web browsers supported 5